УДК 004.021

ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО ПРОДУКТА ДЛЯ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ФАЙЛАМ

А.Г. АНДРЕЙЧИКОВ
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Представлен практический способ создания приложения с использованием криптосистемы, основанной на гибридных алгоритмах шифрования. Результатом работы явилось написание программы для защиты пользовательских файлов с использованием гибридных алгоритмов шифрования, а также создание понятного пользовательского интерфейса. Задача реализации интерфейса решалась с использованием WindowsForm и языка программирования C#.

В настоящий момент самым распространенным способом хранения информации является запись ее на цифровые носители. Часть сохраняемой информации может быть конфиденциальной, приватной, секретной и нуждаться в защите. У такой информации есть законные пользователи. Но всегда существует вероятность появления пользователей незаконных, стремящихся захватить секретную информацию с целью обращения ее себе во благо. Хакеры ежедневно крадут номера кредитных карт, банковские счета и даже личность человека. Опасаясь этого, законные пользователи принимают меры по защите информации.

На сегодняшний день известны несколько подходов к проблеме защиты информации, хранящейся в персональном компьютере. Один из них – шифрование данных.

Принцип разработанного алгоритма защиты информации и его функционал. В качестве симметричного алгоритма шифрования использован алгоритм Triple DES (3DES). Triple DES (3DES) – симметричный блочный шифр, созданный Уитфилдом Диффи, Мартином Хеллманом и Уолтом Тачманном в 1978 году на основе алгоритма DES с целью устранения главного недостатка последнего – малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше. 3DES является простым способом устранения недостатков DES. Алгоритм 3DES построен на основе DES, поэтому для его реализации возможно использовать программы, созданные для DES.

В качестве асимметричного алгоритма шифрования выбран алгоритм RSA, который относится к так называемым асимметричным алгоритмам, у которых ключ шифрования не совпадает с ключом дешифровки. Один из ключей доступен всем и называется открытым ключом, другой хранится только у его хозяина и неизвестен никому другому. С помощью одного ключа можно производить операции только в одну сторону. Если сообщение зашифровано с помощью одного ключа, то расшифровать его можно только с помощью другого. Имея один из ключей, невозможно найти другой ключ, если разрядность ключа высока.

Для аутентификации пользователя используется система логин-пароль. В систему можно зайти с любой комбинацией логина-пароля, однако файлы, зашифрованные с помощью одной комбинации логина-пароля, невозможно дешифровать с помощью другой комбинации, даже введя верный ключ. Данный подход обеспечивает дополнительный уровень защиты от несанкционированного доступа к секретным данным.

Интерфейс программы создан с помощью WindowsForm на языке программирования C# (рис. 1).

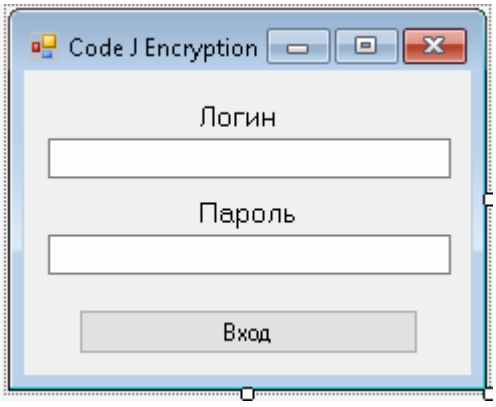

Рисунок 1. – Форма для авторизации в программе

После авторизации в программе и выбора действия интерфейс будет выглядеть, как показано на рисунках 2, 3.

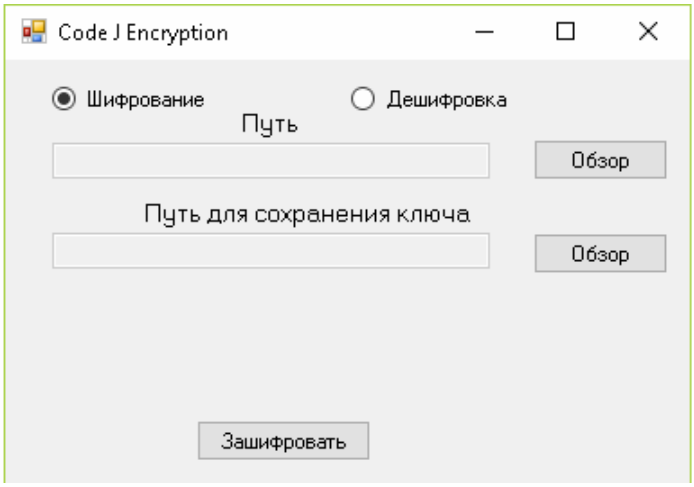

Рисунок 2. – Интерфейс шифрования

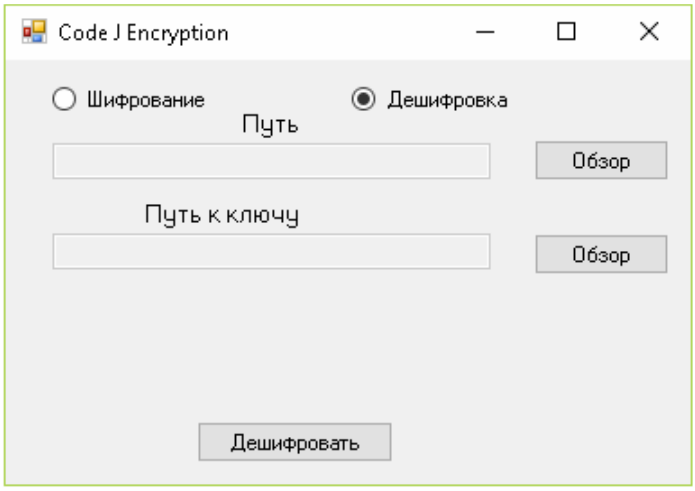

Рисунок 2. – Интерфейс дешифровки

Заключение

Автором разработан программный продукт для надежного хранения конфиденциальной, секретной информации на персональном компьютере. Ведутся работы по увеличению функционала программы и улучшению степени защиты данных.

ЛИТЕРАТУРА

1. Triple DES [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Triple_DES. – Дата доступа: 24.09.2017.
2. Хабрахабр [Электронный ресурс] Пара слов о гибридном шифровании и эллиптических кривых. – Режим доступа: https://habrahabr.ru/post/106057. – Дата доступа: 24.09.2017.
3. Хабрахабр [Электронный ресурс] Немного практической криптографии под .NETдля чайников. – Режим доступа: https://habrahabr.ru/post/254909. – Дата доступа: 24.09.2017.
4. Хабрахабр [Электронный ресурс] RSA, а так ли все просто. – Режим доступа: https://habrahabr.ru/post/99376. – Дата доступа: 24.09.2017.